

TYPO3.Flow - Task # 8427

Status:	Resolved	Priority:	Should have
Author:	Michael Schams	Category:	Security
Created:	2010-06-22	Assigned To:	Andreas Förthner
Updated:	2010-10-20	Due date:	
Sprint:			
PHP Version:			
Has patch:			
Complexity:			
Subject:	Access roles are not inherited		
Description			
<p>Assuming, we defined the following three ACL roles in Policy.yaml:</p> <ul style="list-style-type: none">- administrator- manager- auditor <p>"Auditor" should be the lowest level, "administrator" the highest. A typical example would be: admin has access to everything (incl. user management features), "manager" and "auditor" have access to low level features. Therefore, a good approach would be to inherit all privileges an "auditor" has, to the "manager" role and all privileges a "manager" has, to "administrator".</p> <p>The attached document shows the entries in "Policy.yaml" as an example. Note the two/four lines highlighted in red (at "acl" section). You would expect that you <u>do NOT</u> need those lines, because "manager" already has access to Meter/Asset (inherited by "auditor"), as well as "administrator".</p> <p>But if these lines are removed, an "Access denied" exception is thrown when trying to access Asset/Meters with a "manager" or "administrator" user.</p>			
Assumption:			
Privileges are not inherited. In this example: GRANT for role "auditor" is not passed to "manager" (and "administrator" in the next level).			
Workaround:			
Assign all "admin" users to "auditor" and/or "manager" roles, too. Or: include the additional lines in Policy.yaml as shown in attached document.			

Associated revisions

Revision 45567307 - 2010-06-24 14:54 - Andreas Förthner

- [+BUGFIX] FLOW3 (Security): Inheritance of roles works now again. Fixes #8427.
- [~TASK] FLOW3 (Security): Added a safeguard to catch syntax errors when loading the policy configuration.

History

#1 - 2010-06-22 02:50 - Michael Schams

- File issue8427-FLOW3-policy-issue.pdf added

#2 - 2010-06-23 15:16 - Karsten Dambekalns

- Project changed from Core Team to TYPO3.Flow

#3 - 2010-06-23 15:19 - Andreas Förthner

- Category set to Security
- Status changed from New to Accepted
- Assigned To set to Andreas Förthner

This feature got probably lost in the last refactoring of the security context. The getRoles() method of the context has to take inheritance into account.

I will take care asap.

#4 - 2010-06-24 15:00 - Andreas Förthner

- Status changed from Accepted to Resolved
- % Done changed from 0 to 100

Applied in changeset r4624.

#5 - 2010-07-15 13:36 - Karsten Dambekalns

- Target version set to 1.0 alpha 10

Files

issue8427-FLOW3-policy-issue.pdf	83.4 kB	2010-06-22	Michael Schams
----------------------------------	---------	------------	----------------